06/16/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Christopher E. Mitchell et al.
Title: ENCRYPTION KEY UPDATING FOR MULTIPLE SITE AUTOMATED LOGIN
Attorney Docket No.: 777.395US1

PATENT APPLICATION TRANSMITTAL

BOX PATENT APPLICATION
Commissioner for Patents
Washington, D.C. 20231

We are transmitting herewith the following attached items and information (as indicated with an "X"):

X Return postcard.
X Utility Patent Application under 37 CFR § 1.53(b) comprising:
X Specification (21 pgs, including claims numbered 1 through 42 and a 1 page Abstract).
X Formal Drawing(s) (3 sheets).
X Partially Signed Combined Declaration and Power of Attorney (signed by inventor Christopher E. Mitchell) (3 pgs).
X Preliminary Amendment (1 pg.)

The filing fee (NOT ENCLOSED) will be calculated as follows:

	No. Filed	No. Extra	Rate	Fee
TOTAL CLAIMS	42 - 20 =	22	x 18 =	$396.00
INDEPENDENT CLAIMS	18 - 3 =	15	x 78 =	$1,170.00
[ ] MULTIPLE DEPENDENT CLAIMS PRESENTED				$0.00
BASIC FEE				$690.00
	TOTAL			$2,256.00

THE FILING FEE WILL BE PAID UPON RECEIPT OF THE NOTICE TO FILE MISSING PARTS.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938, Minneapolis, MN 55402 (612-373-6900)

By: _____
Atty: Bradley A. Forrest
Reg. No. 30,837

Customer Number 21186

"Express Mail" mailing label number: EL584210469US Date of Deposit: June 15, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.

By: Shawn L. Hise Signature: _____

S/N Unknown **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Christopher E. Mitchell et al.	Examiner: Unknown
Serial No.:	Unknowr	Group Art Unit: Unknown
Filed:	Herewith	Docket: 777.395US1
Title:	KEY DISTRIBUTION	

Title as Amended Herein: ENCRYPTION KEY UPDATING FOR MULTIPLE SITE AUTOMATED LOGIN

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Prior to examination, please change the title of the above-identified application to read:

--ENCRYPTION KEY UPDATING FOR MULTIPLE SITE AUTOMATED LOGIN--.

Respectfully submitted,

CHRISTOPHER E. MITCHELL ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6972

Date 6-15-2000 By

Bradley A. Forrest
Reg. No. 30,837

Express Mail No.: EL584210469US Mailing Date: June 15, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to Box PATENT APPLICATION, Assistant Commissioner for Patents, Washington, D.C. 20231.

Shawn L. Hise
Printed Name

Signature

Encryption Key Updating for Multiple Site Automated Login

Field of the Invention

This invention relates generally to the field of computers, and in particular to automatically updating keys used to log into multiple sites.

Copyright Notice/Permission

Background

The recent growth in popularity of the Internet has significantly increased the number of Internet users and the number of Internet sites (also referred to as "web sites"). Web sites may provide various types of information to users, offer products or services for sale, and provide games and other forms of entertainment. Many web sites require users to "register" by providing information about themselves before the web server grants access to the site. This registration information may include the user's name, account number, address, telephone number, email address, computer platform, age, gender, or hobbies. The registration information collected by the web site may be necessary to complete transactions (such as commercial or financial transactions). Additionally, information can be collected which allows the web site operator to learn about the visitors to the site to better target its future marketing activities or adjust the information provided on the web site. The collected information may also be used to allow the web site to contact the user

directly (e.g., via email) in the future to announce, for example, special promotions, new products, or new features of the web site.

When registering with a web site for the first time, the web site typically requests that the user select a login ID and an associated password. The login ID allows the web site to identify the user and retrieve the user's information during subsequent user visits to the web site. Generally, the login ID must be unique to the web site such that no two users have the same login ID. The password associated with the login ID allows the web site to authenticate the user during subsequent visits to the web site. The password also prevents others (who do not know the password) from accessing the web site using the user's login ID. This password protection is particularly important if the web site stores private or confidential information about the user, such as financial information or medial records.

If a user visits several different web sites, each web site may require entry of similar registration information about the user, such as the user's name, mailing address, and email address. This repeated entry of identical data is tedious when visiting multiple web sites in a short period of time. Many web sites require the user to register before accessing any information provided on the web site. Thus, the user must enter the requested registration information before they can determine whether the site contains any information of interest.

After registering with multiple web sites, the user must remember the specific login ID and password used with each web site or other Internet service. Without the correct login ID and password, the user must re-enter the registration information. A particular user is likely to have different login IDs and associated passwords on different web sites. For example, a user named Bob Smith may select "smith" as his login ID for a particular site. If the site already has a user with a login ID of "smith" or requires a login ID of at least six characters, then the user must select a different login ID. After registering at numerous web sites, Bob Smith may have a collection of different login IDs, such as: smith, smith1, bsmith, smithb, bobsmith, bob_smith, and smithbob. Further, different passwords may be associated with different login IDs due to

differing password requirements of the different web sites (e.g., password length requirements or a requirement that each password include at least one numeric character). Thus, Bob Smith must maintain a list of web sites, login IDs, and associated passwords for all sites that he visits regularly.

Some sites keep track of this login information for the user, and provide a key ring, which is essentially set of images or icons which when selected provide login information to a site associated.

There is a need for a secure way to log in to multiple sites. There is a further need to be able to change security parameters on sites without interrupting the user or site. There is yet a further need to manage security for multiple sites in a multiple site login service in a simple and uncomplicated manner.

Summary of the Invention

New keys for decrypting automatic login information are distributed, and may coexist with a current key. Following a selected time, the new key becomes the current key.

During the period of coexistence of keys, a multiple site login service which issues the tickets begins to send tickets to the sites which may be decrypted by use of the new key. Following a period of time at least as long as the coexistence period, the old keys are expired and no longer available for use. A configuration file is used to keep track of sites logged into as well as a login ID and password for each site. As a site is visited by the user, the ticket is created from this information. Each key has a version tag associated with it. When an updated key is issued by the login service, the version tag is incremented or otherwise changed.

The site usually has a predetermined reauthorization period, after which each user is required to reauthenticate to the site again. The login service provides the ticket again for reauthorization. By setting the selected time for the new key to become the current key, all users currently logged into a site will not see a difference in operation. By the time the selected time passes, all users

logged into the site will have already reauthorized using a ticket corresponding to the new key.

An individual site may request a new key, as may the login service. In one aspect of the invention, the login service generates a new key for a site to ensure that a minimum level of security of the site is maintained.

Brief Description of the Drawings

Fig. 1 is a block diagram showing pertinent components of a computer in accordance with the invention.

Fig. 2 illustrates an exemplary network environment in which the present invention is utilized.

Fig. 3 is a block diagram showing components involved in key generation, distribution, updating and use.

Detailed Description

In the following detailed description of exemplary embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific exemplary embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical and other changes may be made without departing from the spirit or scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

The detailed description is divided into multiple sections. A first section describes a simple representation of a computer system and the operation of multiple computer systems on a network which implement different aspect of the current invention. This is followed by a description of the invention and how it is implemented.

Hardware and Operating Environment

An exemplary system for implementing the invention includes a computing device, such as computing device 100 in Fig. 1. In its most basic configuration, computing device 100 typically includes at least one processing unit 102 and memory 104. Depending on the exact configuration and type of computing device, memory 104 may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. This most basic configuration is illustrated in Fig. 1 by broken line 106.

Device 100 may also include additional features/functionality. For example, device 100 may include additional storage (removable and/or non-removable) including, but not limited to, magnetic or optical disks or tape. Such additional storage is illustrated in Figure 1 by removable storage 108 and non-removable storage 110. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method of technology for storage of information such as computer readable instructions, data structures, program modules or other data. Memory 104, removable storage 108 and non-removable storage 110 are all examples of computer storage media. Computer storage media includes, but is not limited to RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic based storage or any other medium which can be used to store desired information and which can be accessed by device 100. Any such computer storage media may be part of device 100.

Device 100 may also contain communications connection(s) 112 that allow the device to communicate with other devices. Communications connection(s) 112 is an example of communication media. Communications media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set of changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes

wired media such as wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. The term computer readable media as used herein includes both storage media and communications media.

Device 100 may also have input device(s) 114 such as keyboard, mouse, pen, voice input device, touch input device, etc. Output device(s) 116 such as display, speakers, printers, etc may also be included. All these devices are well known in the art.

This invention may be described in the context of computer-executable instructions, such as program modules, executed by one or more computer or other devices such as device 110. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

Fig. 2 is a block diagram illustrating an exemplary network environment in which the present invention is utilized. A client computer system 200 is coupled to a network 202. In this example, network 202 is the Internet (or the World-Wide Web). However, the teachings of the present invention can be applied to any data communication network that implements a stateless protocol similar to hypertext transfer protocol, http. Multiple affiliate servers 204, 206, and 208 are coupled to network 202, thereby allowing client computer system 200 to access web servers 204, 206, and 208 via the network. Affiliate servers 204, 206, and 208 are also referred to as "web servers", "network servers" and "sites" hosting content such as text and images for access by other computers on the network 202. An authentication server 210 is also coupled to network 202, facilitating communication between the authentication server and client computer system 200 and authentication servers 204, 206, and 208. Although referred to as an "authentication server", authentication server 210 is also a web server capab e of interacting with web browsers and other web servers. In this example, data is communicated between the authentication server 210, client

computer system 200, and web servers using http, a protocol commonly used on the Internet to exchange information. An http specification is published by the Internet Engineering Task Force.

An authentication database 212 is coupled to authentication server 210. The authentication database 212 contains information necessary to authenticate users and also identifies which elements of user profile information should be provided to a particular affiliate server when the user accesses the affiliate server. Although the authentication database 212 is shown separately from the authentication server 210, in other embodiments of the invention, the authentication database is contained within the authentication server.

An authentication process authenticates a user of client computer 200 seeking access to an affiliate server 204, 206, or 208. The authentication server 210 authenticates the user of client computer 200 by requesting authenticating information, such as the user's login ID and password. If the user is successfully authenticated, then authentication server 210 generates an encrypted authentication ticket and communicates the ticket to the appropriate affiliate server. The authentication ticket indicates that the user is authenticated. Each affiliate server requires a key in order to decrypt the ticket and allow access by the user.

The authentication ticket contains two time stamps. The first time stamp indicates the last time that the user's login ID and password were physically typed by the user. The second time stamp indicates the last time that the user's login information was refreshed by the authentication server. This "refresh" of the user's login information can be performed "silently" or by manual entry of the login information (i.e., login ID and password) by the user. The refreshing of the user's login information is performed by the authentication server. Once completed, a new authentication ticket is issued to the affiliate server indicating the new time stamp values.

The term "affiliate server" is defined herein as a web server that has "registered" or established a relationship or affiliation with the authentication server 210. Each affiliate server 204, 206, and 208 includes a code sequence that

allows the affiliate server to communicate with the authentication server 210 when a user (who is also registered with the authentication server) requests access to the affiliate server.

Prior to executing the authentication process, both the user of client computer system 200 and the operator of affiliate server 204 "register" with the authentication server 210. This registration is a one-time process which provides necessary information to the authentication server. The user of client computer system 200 registers by providing information such as the user's email address, password information, and various other information about the user or the client computer system if desired. As part of the user registration process, the user is assigned (or selects) a login ID, which is a common login ID used to access any affiliate server. The login ID may also be referred to herein as a "user name" or "login name". Additionally, the user selects a password associated with the login ID which is used for authentication purposes.

After registering and logging into the authentication server, the user can visit any affiliate server (i.e., affiliate servers that are also registered with the same authentication server) without requiring any additional authentication and without re-entering user information that is already contained in the associated user profile.

The operator of affiliate server 204 registers with the authentication server 210 by providing information about the affiliate server (e.g., server name and internet address). Additionally, the affiliate server provides information regarding its authentication requirements. The authentication requirements can be specified as the maximum time allowed since the last login and entry of authentication information by the user as well as the maximum time allowed since the last "refresh" of the authentication information by the user. Refreshing the authentication information refers to the process of having the user re-enter the password to be certain that the appropriate user is still operating the client computer system. This periodic refreshing of authentication information is useful if the user leaves their computer system without logging out of the authentication server, thereby allowing another individual to access affiliate

servers using the login ID of the previous user. If a user requests access to the affiliate server after the maximum time allowed, then the user is re-authenticated (i.e., refreshed) by the authentication server by issuing a new authentication ticket either silently or with required reentry of password as described above. Thus, although there is a central authentication server, each individual affiliate server can establish its own authentication requirements which are enforced by the authentication server. After registering with the authentication server, the affiliate server can use the authentication server to authenticate any user that has also registered with the authentication server.

A block diagram showing the general operation of key generation and distribution for decrypting tickets is provided in Fig. 3. The authentication server has several servers associated with it. A nexus server 310 manages a configuration file, which contains information regarding partner sites in the form of a partner.xml, information about keys in a keys.xml, and information about the network server in a networkserver.xml in the configuration file. These XML files are each a component configuration document (CCD). Further associated servers include a login server, which provide login services, a register server, and a logout server. Each of these servers may be integrated into a single server, or comprise multiple servers themselves.

A key generator 345 is also associated with the authentication server. It has an administrative interface 350 that allows selection of new keys by a user, and provides keys in the form of an executable piece of code referred to as key.exe via a network 360 (shown in two places for convenience) such as the Internet, to one or more affiliate servers such as a partner site 370. Partner site 370 may have several servers operating as indicated in Figure 3, all servicing the same network domain. The key generator also provides the keys.xml information to the nexus, where it is stored in the configuration file.

When a new partner site is registered by use of the register server 330, a key is generated for the site and provided by S-MIME secure encrypted email, using standard certification, or physically mailed to operators of the site for installation. The key is delivered as an EXE with key data embedded within it.

An object, such as a COM object handles installation and encryption of the keys. The first key has a version number, such as "1", and is stored by the site in encrypted form in a registry using a piece of information that is specific to the physical machine, such as the MAC address of the first network card. The key.exe is used for decrypting tickets while the authentication server is still running.

The administrative interface 350 is used to cause generation of a new siteID for the new partner site, and generation of the key for that site with a one digit Hex version tag or number of "1". Other lengths of version numbers may used as desired. Interface 350 updates the nexus server 310 with information about the partner, such as site ID, keys.xml and current version number. Since there may be multiple trusted servers, i.e.: login servers, each is then triggered to refresh configuration information from the nexus server 310, including the new keys.xml file with the new site's key version "1" included. The keys are distributed as a distinct private secure CCD in clear text over a highly secure (128-bit SSL) channel that is both client and server authenticated. Each time the CCD is retrieved by a trusted server, all the keys are immediately encrypted and stored in a registry, and then the CCD is completely thrown away.

When a new key is to be updated, telephone or email is used to initiate the generation of a new key. Such generation could also be automated if desired. The key may be updated on a regular schedule or variable schedule when initiated on the authentication server side, or may be initiated in accordance with various security protocols on either the authentication server side or partner site side. The partner site administrators may request a new key when an employee leaves, or any time desired.

A new key is then generated at 345 and is updated on the nexus server 310 to add the new key to a list of keys for the partner's siteID in the configuration file. The version number is incremented. When it reaches "F", it loops back to one and resumes incrementing over time.

Key generator 345 also generates a key.exe file that can be installed on the partner site servers. The new key.exe file is sent securely to the partner and

received. The key.exe file is then run against all servers on the partner site with an "/addkey" parameter that installs the new key onto the server while still running. It is added as an additional key with no expiration date.

Next, the partner site runs the key.exe file against all servers with a "/makecurrent" parameter to make the new key the current key by switching a registry key referred to as keycurrent to the new key version. They registry my also take the form of a config file, or any file in other systems. It also sets an expiration date on the previous current key equal to the current time plus a registry key value referred to as TimeWindow. Time window may be set equal to the reauthorization time, or any other desired time. It may also be set to zero to immediately begin exclusive use of the new current key to access the partner site. If no time window has been set, old keys are flushed every 24 hours or so if desired.

Key.exe may also be run against all servers using an "/expire" parameter prior to receiving a new key to cause a service interruption until new keys are installed. This ensures that no new tickets using an old compromised key are accepted, and the old key can be immediately deleted from all servers.

The manager at each site 370 uses several registry keys to keep track of encryption keys. A SiteID is the partner site's ID and is used in all calls to the authentication server. A TimeWindow is essentially the site's default preference for how "fresh" a user's ticket must be before they are redirected back to the login server for a new key. KeyData contains the actual keys, encrypted in the HMAC of the machine. Each encryption key is stored as a value of this registry key, with the version stamp as the value's name, and the encrypted key data as the value's data. These values map one to one with values under KeyTimes. KeyTimes specifies the expiration dates of all the keys referenced in KeyData. For each encryption key, this registry key will contain a value whose name is the encryption key's version stamp, and whose data is the date and time at which this key is no longer valid. The value "-1" signifies that the key never expires. Typically, keys are set to never expire until it is time to update the key. CurrentKey is the version stamp of the current key. The version stamp is

referenced in all requests to authentication servers. It indicates which key this server expects to get new tickets in.

When there is a new key, users that are currently logged on will be able to continue their session using the old key. When KeyTimes expires, they must use the new key to reauthorize their session. When this happens, or when a new user attempts to log in with an older version ticket after key.exe has been run with MakeCurrent, the partner site receives an attempt to log in by the user using the old ticket. When parsing a ticket with an expired key, it is rejected, the user gets redirected to the login server URL with parameters "ID=xxx&KV=2" used to specify the new encryption key. The user is redirected by this URL to the login server. This redirection causes the login server to update the configuration file to indicate that the new key is now the current key.

A new ticket is generated using the new key. As each new user or reauthorization request is received for that site, the new current key will be used to generate the ticket. In its unencrypted form, the ticket sent by the user comprises authentication time stamps and user information. When encrypted, it takes the form of: "keyversion#, string", where the string is an encrypted form of the timestamps and user information.

Conclusion

The key generation and distribution process provides a safe, reliable way of distributing keys to partner sites that requires minimal human intervention, little if any user disruption, and minimal operational disruption. While parts of the process have been described in terms of human operations, these operations may be easily automated. In the same manner, automated operations may also be performed by human actions. The process allows two keys to be operative for a desired amount of time.

We claim:

1. A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;

generating a second key having a second version number; and

when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number.

2. The method of claim 1 wherein a different key is provided to each site, and wherein each key is encrypted for decoding at one site.

3. The method of claim 1 and further including generating a configuration file to track keys for each site.

4. The method of claim 1 wherein the key comprises key data and executable code for decrypting tickets.

5. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;

generating a second key having a second version number; and

when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number.

6. A method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key in the form of an executable having a first version number;

generating a second key in the form of an executable having a second version number; and

providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

7. The method of claim 6 and further comprising distributing the key to multiple login servers in a secure manner.

8. The method of claim 6 and further comprising updating a configuration file to track keys for each site.

9. A computer readable medium having instructions stored thereon for causing a computer to perform a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key in the form of an executable having a first version number;

generating a second key in the form of an executable having a second version number; and

providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

10. A system that generates keys that decrypt login tickets that log a user into multiple sites, the system comprising:

a key generator that generates a first key in the form of an executable having a first version number and generates a second key in the form of an executable having a second version number; and

means for providing information to a login server identifying which key is current for each site such that the tickets are properly encoded.

11. A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a new key with an incremented version number;

sending the new key to a partner site for use in decoding tickets with the incremented version number;

updating key and version information for a login server; and

generating tickets decodable by the new key when an indication that a key having a previous version number has expired.

12. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a new key with an incremented version number;

sending the new key to a partner site for use in decoding tickets with the incremented version number;

updating key and version information for a login server; and

generating tickets decodable by the new key when an indication that a key having a previous version number has expired

13. A method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire;

making the updated key the current key.

14. The method of claim 13 wherein the key comprises executable code for making the updated key the current key.

15. The method of claim 13 and further comprising redirecting users attempting to log into the site using the old current key.

16. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire;

making the updated key the current key.

17. A method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire; and

making the updated key the current key.

18. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire; and

making the updated key the current key.

19. A method of managing keys used to decrypt tickets for logging onto a site, the method comprising:

receiving a first key with a first version number;

encrypting the first key using a hardware address;

changing a current key variable to the first version number;
receiving a new key with an incremented version number;
encrypting the new key using a hardware address; and
identifying the new key as the current key.

20. Them method of claim 19 and further comprising setting a time for the first key identifying when such key may no longer be used.

21. The method of claim 20 wherein a user currently logged in may continue to use the first key until the time expires.

22. The method of claim 20 wherein new user may only use a ticket corresponding to the second key when the second key is made the current key.

23. The method of claim 20 wherein the time is set to a reauthorization time determined by the site.

24. The method of claim 19 wherein a new user using a previous version ticket will be redirected to obtain a ticket corresponding to the new key following the new key being identified as the current key.

25. The method of claim 19 wherein the new key is identified as the current key by changing the current key variable to the second version number.

26. A computer readable medium having instructions stored thereon for causing a computer to perform a method of managing keys used to decrypt tickets for logging onto a site, the method comprising:
receiving a first key with a first version number;
encrypting the first key using a hardware address;
changing a current key variable to the first version number;
receiving a new key with an incremented version number;

encrypting the new key using a hardware address; and

identifying the new key as the current key.

27. A method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising:

generating a new key with a new version number to take the place of an old key with an old version number;

storing the new key on a site to be logged into by a user;

changing a current key indication to the new key;

allowing current logged in users to continue using the old key; and

redirecting new users to a login server to obtain a ticket consistent with the new key.

28. The method of claim 27 wherein the old key may be used by current logged in users for a predetermined amount of time.

29. The method of claim 28 wherein the predetermined amount of time is no more than a reauthorization time by which a current user is normally required to provide login information.

30. The method of claim 28 wherein the predetermined amount of time may be set to zero to force all current and new users to login with a ticket consistent with the new key version.

31. The method of claim 27 wherein the ticket contains a version number consistent with the version number of the key which can decrypt it.

32. The method of claim 27 wherein keys are encrypted by the site using a hardware address, and stored by the site.

33. The method of claim 27 wherein a new key is generated based on a request of the site.

34. The method of claim 27 wherein keys are generated in an executable form which includes key information as well as code for decrypting tickets using the key information.

35. The method of claim 27 wherein the keys are generated by an authentication server, and are distributed to multiple login servers for providing login tickets.

36. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising:

generating a new key with a new version number to take the place of an old key with an old version number;

storing the new key on a site to be logged into by a user;

changing a current key indication to the new key;

allowing current logged in users to continue using the old key; and

redirecting new users to a login server to obtain a ticket consistent with the new key.

37. A method of logging on to multiple sites, the method comprising:

sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;

receiving an indication that the first key has expired;

obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and

sending the second login ticket to the site to log into the site.

38. The method of claim 37 wherein the tickets contain a version number which is readable without decryption.

39. The method of claim 38 wherein the version number is a one digit Hex integer.

40. The method of claim 38 wherein the encrypted ticket comprises an unencrypted version number, and encrypted information sufficient to log a user into a desirec site.

41. A computer readable medium having instructions stored thereon for causing a computer to perform a method of logging on to multiple sites, the method comprising:

sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;

receiving an indication that the first key has expired;

obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and

sending the second login ticket to the site to log into the site.

42. An encrypted ticket for use in logging on to a website, the ticket comprising:

an unencrypted version number corresponding to a key version number stored on the website; and

an encrypted string identifying the website and information, which when decrypted using the key having the same version number authenticates the user for logging the user into the website.

Abstract of the Disclosure

A version number is associated with an encrypted key executable to allow real time updating of keys for a system which facilitates users signing on to multiple websites on different domains using an encrypted ticket. Two keys may be used at each site during updating of keys, each having an associated one digit Hex version tag. When a key is to be updated with a new key, the existing or old key is provided an expiration time. A second key is provided from the system in a secure manner with a new version number and made the current key which provides decryption of the encrypted ticket. The system tracks both keys while they are concurrent. After the existing key expires, only the second, or updated key is used to provide login services for users. The system periodically flushes old keys.

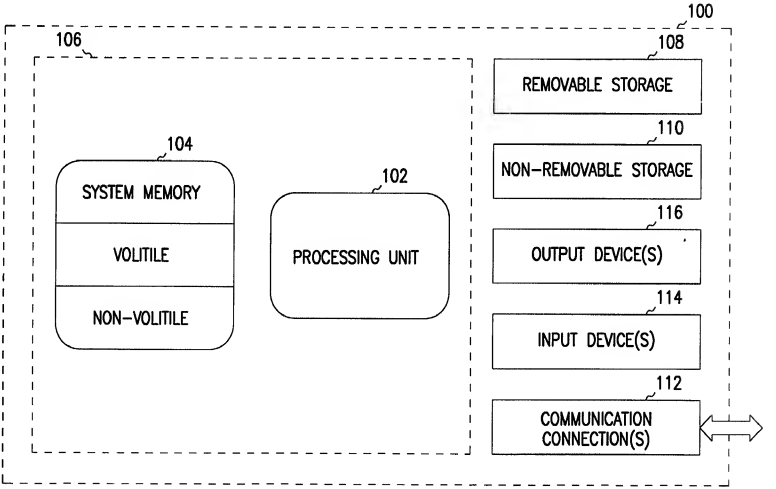

FIG. 1

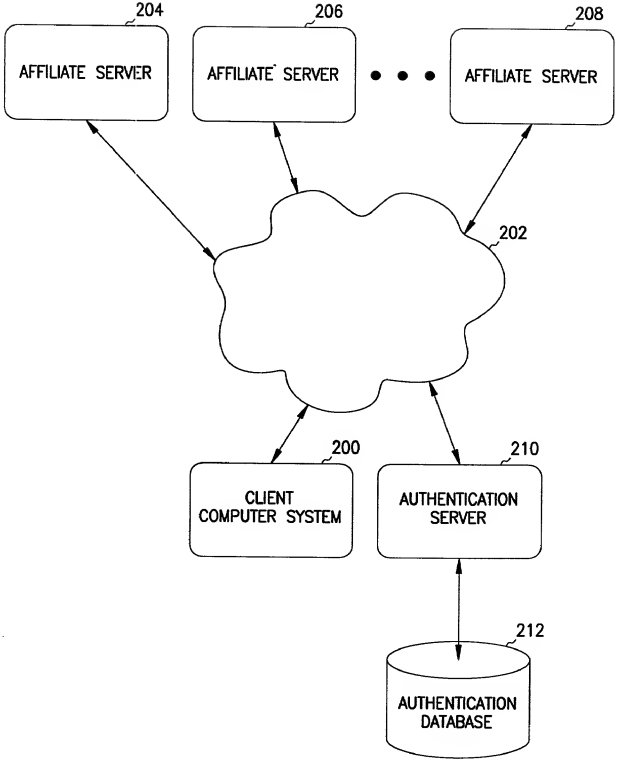

FIG. 2

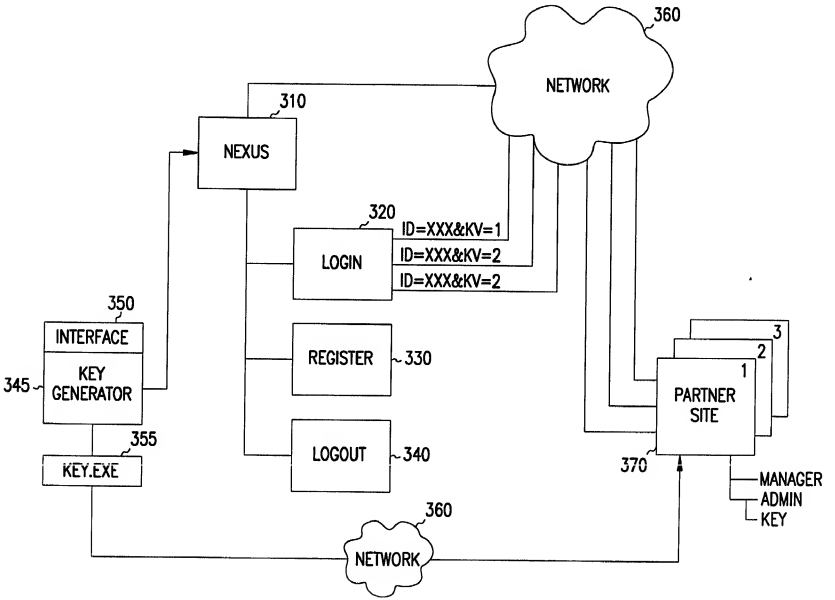

FIG. 3

SCHWEGMAN ■ LUNDBERG ■ WOESSNER ■ KLUTH

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **KEY DISTRIBUTION**.

The specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 C.F.R. § 1.56 (attached hereto). I also acknowledge my duty to disclose all information known to be material to patentability which became available between a filing date of a prior application and the national or PCT international filing date in the event this is a Continuation-In-Part application in accordance with 37 C.F.R. §1.63(e).

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on the basis of which priority is claimed:

No such claim for priority is being made at this time.

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

No such claim for priority is being made at this time.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

No such claim for priority is being made at this time.

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Anglin, J. Michael	Reg. No. 24,916	Huebsch, Joseph C.	Reg. No. 42,673	Nelson, Albin J.	Reg. No. 28,650
Bianchi, Timothy E.	Reg. No. 39,610	Jurkovich, Patti J.	Reg. No. 44,813	Nielsen, Walter W.	Reg. No. 25,539
Billion, Richard E.	Reg. No. 32,836	Kalis, Janal M.	Reg. No. 37,650	Oh, Allen J.	Reg. No. 42,047
Black, David W.	Reg. No. 42,331	Kaufmann, John D.	Reg. No. 24,017	Padys, Danny J.	Reg. No. 35,635
Brennan, Leonicde M.	Reg. No. 35,832	Klima-Silberg, Catherine I.	Reg. No. 40,052	Parker, J. Kevin	Reg. No. 33,024
Brennan, Thomas F.	Reg. No. 35,075	Kluth, Daniel J.	Reg. No. 32,146	Perdok, Monique M.	Reg. No. 42,989
Brooks, Edward J., III	Reg. No. 40,925	Lacy, Rodney L.	Reg. No. 41,136	Prout, William F.	Reg. No. 33,995
Chu, Dinh C.P.	Reg. No. 41,676	Lemaire, Charles A.	Reg. No. 36,198	Sako, Katie E.	Reg. No. 32,628
Clark, Barbara J.	Reg. No. 38,107	LeMoine, Dana B.	Reg. No. 40,062	Schumm, Sherry W.	Reg. No. 39,422
Crouse, Daniel D.	Reg. No. 32,022	Lundberg, Steven W.	Reg. No. 30,568	Schwegman, Micheal L.	Reg. No. 25,816
Dahl, John M.	Reg. No. 44,639	Mack, Lisa K.	Reg. No. 42,825	Smith, Michael G.	Reg. No. 45,368
Drake, Eduardo E.	Reg. No. 40,594	Maeyaert, Paul L.	Reg. No. 40,076	Speier, Gary J.	Reg. No. 45,458
Embretson, Janet E.	Reg. No. 39,665	Maki, Peter C.	Reg. No. 42,832	Steffey, Charles E.	Reg. No. 25,179
Fordenbacher, Paul J.	Reg. No. 42,546	Malen, Peter L.	Reg. No. 44,894	Terry, Kathleen R.	Reg. No. 31,884
Forrest, Bradley A.	Reg. No. 30,837	Mates, Robert E.	Reg. No. 35,271	Tong, Viet V.	Reg. No. 45,416
Garnon, Owen J.	Reg. No. 36,143	McCrackin, Ann M.	Reg. No. 42,858	Viksnins, Ann S.	Reg. No. 37,748
Harris, Robert J.	Reg. No. 37,346	Nama, Kash	Reg. No. 44,255	Woessner, Warren D.	Reg. No. 30,440

☐ I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization/who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Schwegman, Lundberg, Woessner & Kluth, P.A. to the contrary.

Please direct all correspondence in this case to **Schwegman, Lundberg, Woessner & Kluth, P.A.** at the address indicated below:

P.O. Box 2938, Minneapolis, MN 55402
Telephone No. (612)373-6900

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of joint inventor number 1 : **Christopher E. Mitchell**
Citizenship: **United States of America** Residence: **Redmond, WA**
Post Office Address: 516 240th Avenue SE
Redmond, WA 98053

Signature: _____ Date: 6/9/00
Christopher E. Mitchell

Full Name of joint inventor number 2 : **Jeff C. Kunins**
Citizenship: **United States of America** Residence: **San Francisco, CA**
Post Office Address: 23 Roscoe Street
San Francisco, CA 94110

Signature: _____ Date: _____
Jeff C. Kunins

X Additional inventors are being named on separately numbered sheets, attached hereto.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of joint inventor number 3 : **Max E. Metral**
Citizenship: Residence:
Post Office Address:

Signature: _____ Date: _____
Max E. Metral

Full Name of inventor:
Citizenship: Residence:
Post Office Address:

Signature: _____ Date: _____

Full Name of inventor:
Citizenship: Residence:
Post Office Address:

Signature: _____ Date: _____

Full Name of inventor:
Citizenship: Residence:
Post Office Address:

Signature: _____ Date: _____

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.